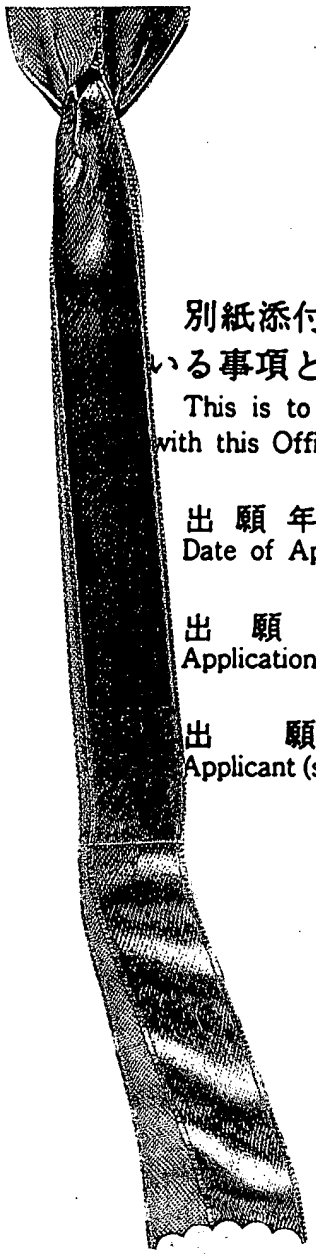


日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１２月２８日

出願番号
Application Number: 平成１１年特許願第３７４９２３号

出願人
Applicant (s): 日本アイ・ビー・エム株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ５月１２日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０３４１５０

【書類名】　特許願

【整理番号】　JA999745

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 12/00

【発明者】

【住所又は居所】　東京都中央区日本橋箱崎町１９番地１　日本アイ・ビー・エム株式会社　箱崎事業所内

【氏名】　佐藤　嘉宏

【特許出願人】

【識別番号】　592073101

【住所又は居所】　東京都港区六本木３丁目２番１２号

【氏名又は名称】　日本アイ・ビー・エム株式会社

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【連絡先】　０４６２－７３－３３１８、３３２５、３４５５

【選任した代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【手数料の表示】

【予納台帳番号】　029193

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9306921

【包括委任状番号】　9306922

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】アクセス制御機構を備えたデータ処理システム

【特許請求の範囲】

【請求項１】

複数ユーザ間で使用される共有データへのアクセスを制御する機構を備えたデータ処理システムであって、

上記共有データを格納するデータ格納手段と、

上記共有データへのアクセス権を制御するためのアクセス管理情報を含むアクセス管理テーブルと、

アクセス対象となる上記共有データへのアクセス付与権限を有する第１のユーザから第２のユーザへの当該データに対する参照を含む通信に応答して、上記アクセス管理テーブルのアクセス管理情報を更新する制御手段と、

を具備するデータ処理システム。

【請求項２】

上記アクセス管理テーブルのアクセス管理情報が、アクセス対象となるデータの識別情報、アクセスを付与される第２のユーザの識別情報およびアクセス・レベル情報を含む、請求項１記載のデータ処理システム。

【請求項３】

上記アクセス管理テーブルのアクセス管理情報が、さらにアクセスを付与する第１のユーザの識別情報を含む、請求項２に記載のデータ処理システム。

【請求項４】

上記制御手段が、上記通信の際にユーザ側から発行されるコマンドに応答してアクセス管理情報を更新する、請求項１ないし３のいずれか１に記載のデータ処理システム。

【請求項５】

請求項１ないし４のいずれか１に記載のデータ処理システムと、当該データ処理システムと通信する複数のユーザ端末とを具備する、データ通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークを介して複数のユーザ間でデータを共有するためのデータ処理システムに係り、特に、そのようなデータへのアクセス権限の付与を簡便に行なうためのデータ処理システムに関する。

【０００２】

【従来の技術】

インターネットやグループウェアといった環境の発達にともない、個人のみならず企業においても様々な業務処理において電子的なデータのやり取りが増加している。例えば、伝票や各種の帳票、契約書等を電子化し、一定範囲のユーザ間でかかる電子化されたデータを送受する等の場合であり、そのような電子的データの多くは利便性のため複数のユーザ間で共有される。このようにデータを共有化する場合、無権限者によるデータの不正利用を防ぐため、データ保護の観点からのアクセス管理が必要になる。

【０００３】

通常は、データへのアクセス権を制御する担当者（「管理者」という）により適切なアクセス管理が行なわれる。例えば、ある文書ファイルを作成したオリジナルの作成者または当該作成者等からアクセス許可の権限を付与された者（まとめて「許可者」という）は、管理者に対しその文書ファイルを利用できるユーザの範囲を指定する（ただし、許可者が同時に管理者となることもある）。その後、指定されたユーザの範囲を管理者が事前にシステムに設定することにより、ユーザが当該文書ファイルにアクセスすることが可能となる。すなわち、ユーザは、所望の共有データを参照するための参照情報を連絡されるだけではなく、管理者を通じた許可者によるアクセス権の付与が行なわれた後にはじめて、当該データを参照できるようになる。

（なお、以下で「参照情報を連絡（通信、通知等）」するというときは、データ本体そのものを送信するのではなく、そのデータにアクセスするために必要な情報のみを送信することを意味する。具体的な態様は、利用するアプリケーションの機能によっても異なるが、例えば、ロータス社のグループウェア製品であるＮＯＴＥＳシステムにおいてデータベース・アイコンを電子メール中に作成して送

付する場合等がこれに相当する。）

【０００４】

また、同一のデータについてのアクセス権の付与権限が複数の者に与えられている場合がある。この場合には、どの権限者も同様に任意のユーザにデータへのアクセス権の付与が可能である。したがって、あるユーザに付与されたアクセス権限が誰によって付与したのかを後にトレースしようとしても、その特定は困難であることが多い。

【０００５】

【発明が解決しようとする課題】

実社会においては、他者に対してある書類を渡した時点で、その書類に対するアクセス権を付与したと考えることができる。例えば、ある書類をその作成者であるＡさんがＢさんに渡した場合、ＡさんはＢさんにその書類を見てよいということを許可し（＝アクセス権の付与）、その結果Ｂさんはその書類を見ることができるようになる（＝実際のアクセス、参照）。すなわち、実際の社会では、データへのアクセス権の付与と参照が同時に行えるようになっている。しかしながら、従来のデータ処理の方式では、上述のようにユーザにデータへの参照情報を連絡する前に、別途事前にアクセス権の付与作業を行う必要がある。すなわち、従来のデータ処理システムでは、事前のアクセス権限の付与手続が必要となる分、現実よりも１ステップ余分の処理を要するという問題がある。

【０００６】

また、実社会では書類自体の入手経路をたどることでアクセス権限を付与した履歴を把握できることがある。しかしながら、従来のデータ管理方式ではアクセス権を付与した記録を残さないか、あるいは残していてもデータ全体に対して時系列のログとして記録しているため、誰がアクセス権限を付与したかという履歴の把握が困難であるという問題がある。

【０００７】

【課題を解決するための手段】

本発明は、上記の問題を解決すべくなされたものであり、もっとも典型的には、共有データに対する参照情報を許可者が電子メール等で他のユーザに通信した時

点で、対象となる共通データ、アクセスを許可されるユーザ名等の情報を自動取得し、アクセス権を付与するためのコマンドを自動発行するなどして、ユーザ間の通信において自動的にアクセス管理情報の更新が行なえるようにする。アクセスを管理するシステムには、アクセス権を管理するためのアクセス管理テーブルとこれを処理するための制御部が設けられており、上記のコマンド等に応答して自動的にテーブルの値を設定する。付与されるアクセス権は、標準値（デフォルト値）や許可者による事前の設定値により、様々なアクセスレベル（ＲＥＡＤのみ等）で設定することが可能である。また、メール等を送信した発行者＝許可者の情報も自動入手し、該当データに対して誰がアクセス許可をしたかのデータもアクセス管理テーブルに保管する構成とすることで、データの入手経路の把握も容易になる。

【０００８】

より具体的には、本発明は、複数ユーザ間で使用される共有データへのアクセスを制御する機構として、かかる共有データを格納するためのデータ格納手段と、上記共有データへのアクセス権を制御するためのアクセス管理情報を含むアクセス管理テーブルと、アクセス対象となるデータへの参照を含むアクセス許可ユーザからの通信に応答してアクセス管理情報を更新する制御手段とを具備するデータ処理システムにより実現される。

【０００９】

上記アクセス管理テーブルのアクセス管理情報としては、アクセス対象となるデータの識別情報、アクセスを付与されるユーザの識別情報、アクセス・レベル情報、アクセスを付与するユーザの識別情報を含みうる。上記の制御手段は、通信の際にユーザ側から発行されるコマンドに応答してアクセス管理情報を更新する構成にすることで処理をより簡便に行なうことができる。

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて説明する。図１は、本発明のデータ処理システムを含む通信システムの構成を説明するブロック図である。図１において、本発明におけるサーバ装置１０は、データ格納部１１、テーブル格納部１３および制御部１５を具備している。データ格納部１１は共有データ１２そ

の他のデータを格納している。サーバ装置１０がメールサーバとしても機能する場合には、各ユーザ毎のメール・データを有することもできる。テーブル格納部１３はデータに対するアクセス情報を制御するためのテーブルであるアクセス管理テーブル１４などの制御用の各種テーブルを格納している。制御部１５は、クライアント・システムとしても機能するユーザ端末１６からの処理要求に応じて、データ格納部１１中のデータの処理や、テーブル格納部１４中のテーブル情報の追加、削除、更新等を行なう。また、サーバ装置１０がメールサーバとしても機能する場合には、所定のメール操作も行なう。図１では、図を簡単にするため、ユーザ端末１６が２台しか示されていないが、実際にはこれ以上の数の端末がＬＡＮ、インターネットまたは他のネットワークを介して接続されている。また、本図では、クライアント-サーバ・モデルのシステムとして構成しているが、他のシステム構成としてもよい。さらに本図では、データ格納部１１とテーブル格納部１４が別々に示されているが、単一の装置としてこれらを構成してもよいし、また分散モデルのようにさらに複数の装置としてこれらを構成してもよい。また、制御部１５は、サーバ装置１０の側に設けられているが、テーブル等の操作権限を有するのであれば、それ以外の装置（例えばクライアント側の端末）に設けてもよい。

【００１０】

ユーザ端末１６を用いる特定のユーザまたはグループは、アクセス管理テーブル１４に許可された範囲で共有データ１２にアクセスすることができる。このようなアクセス管理は、制御部１５において行われる。例えば、ユーザＢがあるデータＸにアクセスしようとすると、サーバ装置１０の制御部１５はアクセス管理テーブル１４の内容を確認し、データＸに対するユーザＢのアクセス権限がある場合にはこれを許可し、ない場合にはこれを拒否する。アクセス管理テーブル１４の内容は、通常は、対象となるデータのアクセス権を決定できる許可者（当該データの作成者等）またはその管理者によりあらかじめ設定される。

【００１１】

本発明においては、このアクセス管理テーブル１４の更新が、許可者から所定のユーザへの電子メール等の送信時に自動的に行えるようにする。したがって、許

可者による（または管理者を通じての）事前のテーブル更新が不要になる。これを図１を用いて具体的に説明する。まず、ユーザＡが特定のデータＸについて許可者としての権限を有する者であり、ユーザＢへの電子メールの送信時に参照するデータＸへのアクセス権がユーザＢに付与されるものとする。この場合、ユーザＡが作成したユーザＢ宛ての電子メールには参照するデータＸに関する記述（参照情報）が含まれており、対象データがユーザＢに連絡される。本発明では、そのメールの送信時にアクセス管理テーブル１４の内容を更新するコマンド（テーブル更新コマンド）が作成され発行される。このコマンドは、対象となるデータ（Ｘ）、アクセス許可されるユーザ（Ｂ）、アクセスの許可者（Ａ）、その許可レベル（ＲＥＡＤのみ等）等をパラメータとして含むことができる。このテーブル更新コマンドに応答して、制御部１５はテーブル１４の内容を書き換え、その結果、ユーザＢにデータＸに対するアクセス権が付与される。ユーザＢはユーザＡからのメールを受け取った時点でデータＸに対するアクセス権をすでに取得しているので、その後、メール中の参照情報をもとにデータＸへアクセスすることが可能となる。

【００１２】

上記においては、電子メールの送付時にユーザ端末側でコマンドを作成、発行する構成としたが、単にユーザ要求の指定に基づき、サーバ側の制御部で所定のテーブル更新を行なう構成としてもよい。例えば、サーバ装置１０がメールサーバとしても機能するような場合に、メール送信時のユーザ側の指定に基づき、単に対応するテーブル処理を実行するような構成とすることもできる。

【００１３】

図２は、共有データに対するアクセス権を判定するためのアクセス管理テーブルを説明する図である。図２において、欄２１はデータ毎に付与されるユニークなデータ識別子、欄２２は各データについてアクセス権レベルを設定されているユーザ又はグループ名、欄２３は個々のユーザ等に設定されたアクセス権レベル、欄２４は個々のユーザに対してアクセス権を付与した許可者のユーザ名を表す。データの作成者はアクセス権を他者から付与されないので、欄２４には何も入力しないかまたはユーザＩＤ欄２２と同一のユーザ名を入力することになる。ある

データに対する参照情報を上記のように他者に連絡した場合、該当する連絡をしたユーザが許可者欄２４に、連絡を受けたユーザがユーザＩＤ欄２２の項目に設定される。なお、アクセス権を付与した履歴が特に必要がないシステムにおいては、アクセス管理テーブルの許可者欄は省略可能である。また、図２の権限欄２３では、単に「ＷＲＩＴＥ／ＤＥＬ」（書込み・削除可能）、「ＲＥＡＤ」（読取り可能）の２種類のみの設定としたが、さらに他者へのデータの転送（ＦＯＲＷＡＲＤ）を認めるかどうかを設定するパラメータ等、他の任意の設定を同欄に含めてもよい。この場合、特に指定がなければデフォルトの既定値として、例えば「ＲＥＡＤ」（ＦＯＲＷＡＲＤ不可）を設定し、特に送信時の設定がある場合には、その任意の値に設定するよう構成することができる。

【００１４】

図３は、本発明によるデータのアクセス制御の方法を説明するフロー図である。図３の処理は、主に制御部１５において実行される。まず、ユーザ端末１６からのユーザ要求に基づき、特定のユーザまたはグループに対する通信またはメールの送信において、共有データ１２に対する参照情報を含むかが判断される（ステップ３１）。上述のように、所定のパラメータを含むコマンドが発行される場合には、そのコマンドにより参照処理が必要であることが判断され、パラメータ情報が共有データに対する具体的な参照情報として機能する。参照処理がある場合には、ステップ３２に進む。ステップ３２においては、アクセス管理テーブル１４の内容を検査し、通信等の宛先ユーザに対して既にアクセス権が付与されているかを判断する。ステップ３３で、アクセス権が既に付与されている場合には特に処理を行なうことはないが、アクセス権がない場合には、アクセス管理テーブル１４に、図２に示すようなデータＩＤ２１、ユーザＩＤ２２、権限２３、許可者２４をユーザ要求の参照情報に基づき設定する。これにより、メールの送信時にその送信先に対するアクセス権の付与が行われるとともに、アクセス権付与の履歴を残すことができるようになる。

【００１５】

【発明の効果】

以上説明したように、本発明によれば、特定のユーザまたはグループの特定のデ

ータに対するアクセス制御を、容易な操作で行なうことが可能となり、業務の操作性が高まる。また、アクセス権限の付与者（許可者）のデータを明確に保管することで、データの入手経路を容易に確認することができるようになる。

【図面の簡単な説明】

【図１】本発明のデータ処理システムを含むシステム構成を説明するブロック図である。

【図２】共有データに対するアクセス権を判定するためのアクセス管理テーブルを説明する図である。

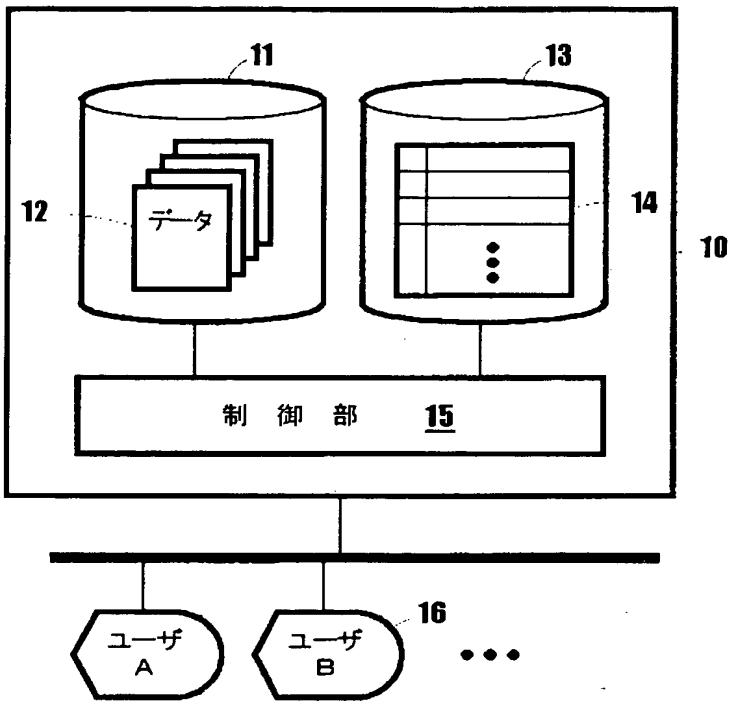
【図３】本発明によるデータのアクセス制御の方法を説明するフロー図である。

【符号の説明】

１０・・・サーバ装置、１１・・・データ格納部、１２・・・共有データ、１３・・・テーブル格納部、１４・・・アクセス管理テーブル、１５・・・制御部、１６・・・ユーザ端末

【書類名】　図面

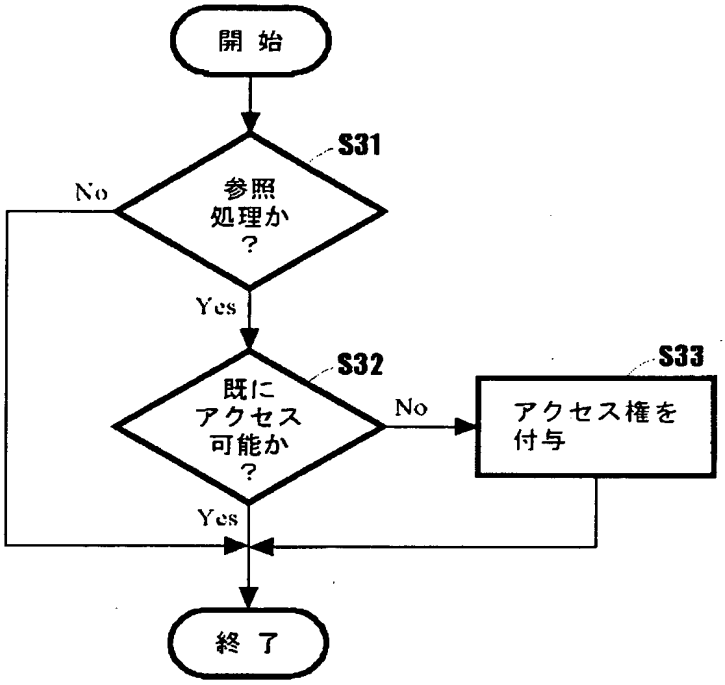
【図１】



【図２】

21 データＩＤ	22 ユーザＩＤ	23 権　限	24 許可者
0001	UserA	WRITE/DEL	－(作成者)
0001	UserB	READ	UserA
0001	UserC	READ	UserB
⋮	⋮	⋮	⋮
nnnn	xxxx	wwww	yyyy

【図３】



【書類名】　要約書

【要約】

【課題】

ネットワークを介して複数のユーザ間でデータを共有する環境で、そのようなデータへのアクセス権限の付与を簡便に行なうためのデータ処理システムを提供する。

【解決手段】

本発明は、複数ユーザ間で使用される共有データへのアクセスを制御する機構として、かかる共有データを格納するためのデータ格納手段と、上記共有データへのアクセス権を制御するためのアクセス管理情報を含むアクセス管理テーブルと、アクセス対象となるデータへの参照を含むアクセス許可ユーザからの通信に応答してアクセス管理情報を更新する制御手段とを具備するデータ処理システムにより実現される。アクセス管理テーブルのアクセス管理情報としては、アクセス対象となるデータの識別情報、アクセスを付与されるユーザの識別情報、アクセス・レベル情報、アクセスを付与するユーザの識別情報を含みうる。

【選択図】

図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第３７４９２３号
受付番号	５９９０１２８４６１５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　１月　５日

＜認定情報・付加情報＞

【提出日】　平成11年12月28日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５９２０７３１０１〕

１．変更年月日　　１９９２年　４月　３日
［変更理由］　新規登録
住　所　東京都港区六本木３丁目２番１２号
氏　名　日本アイ・ビー・エム株式会社